FIG.1

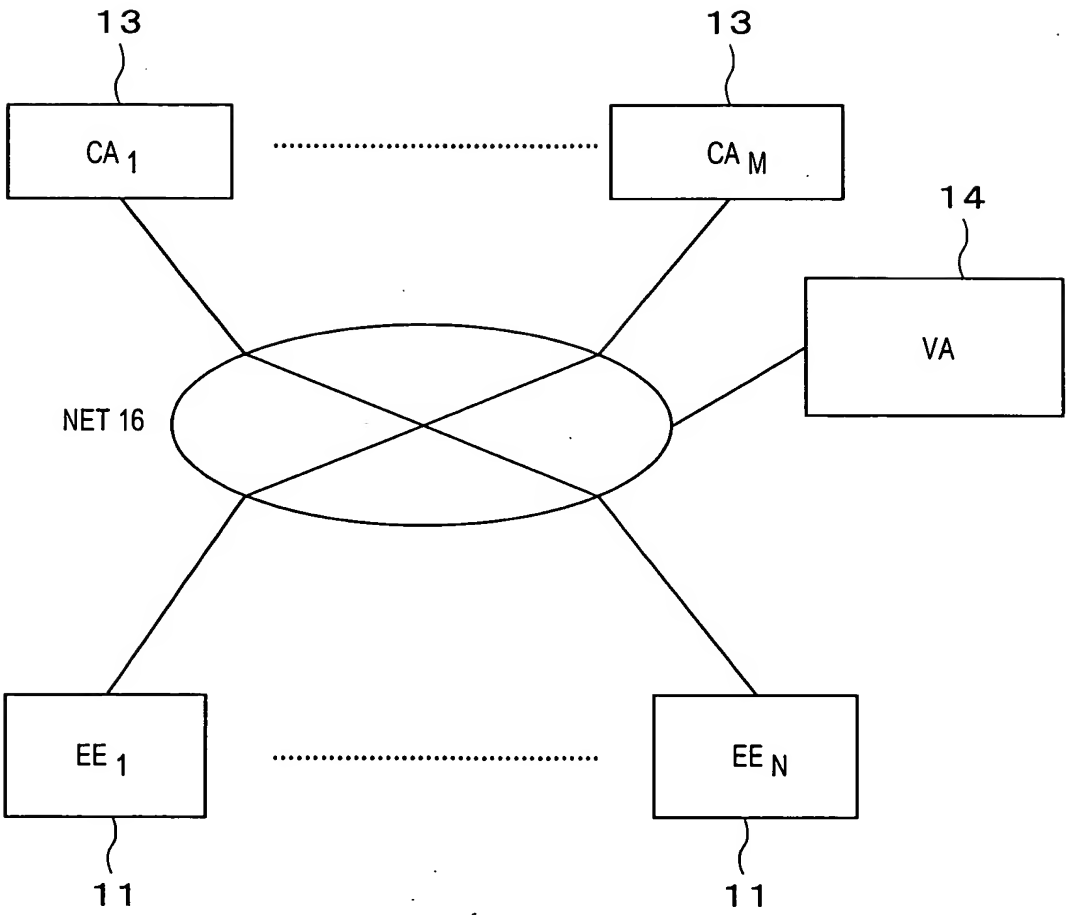


FIG.2

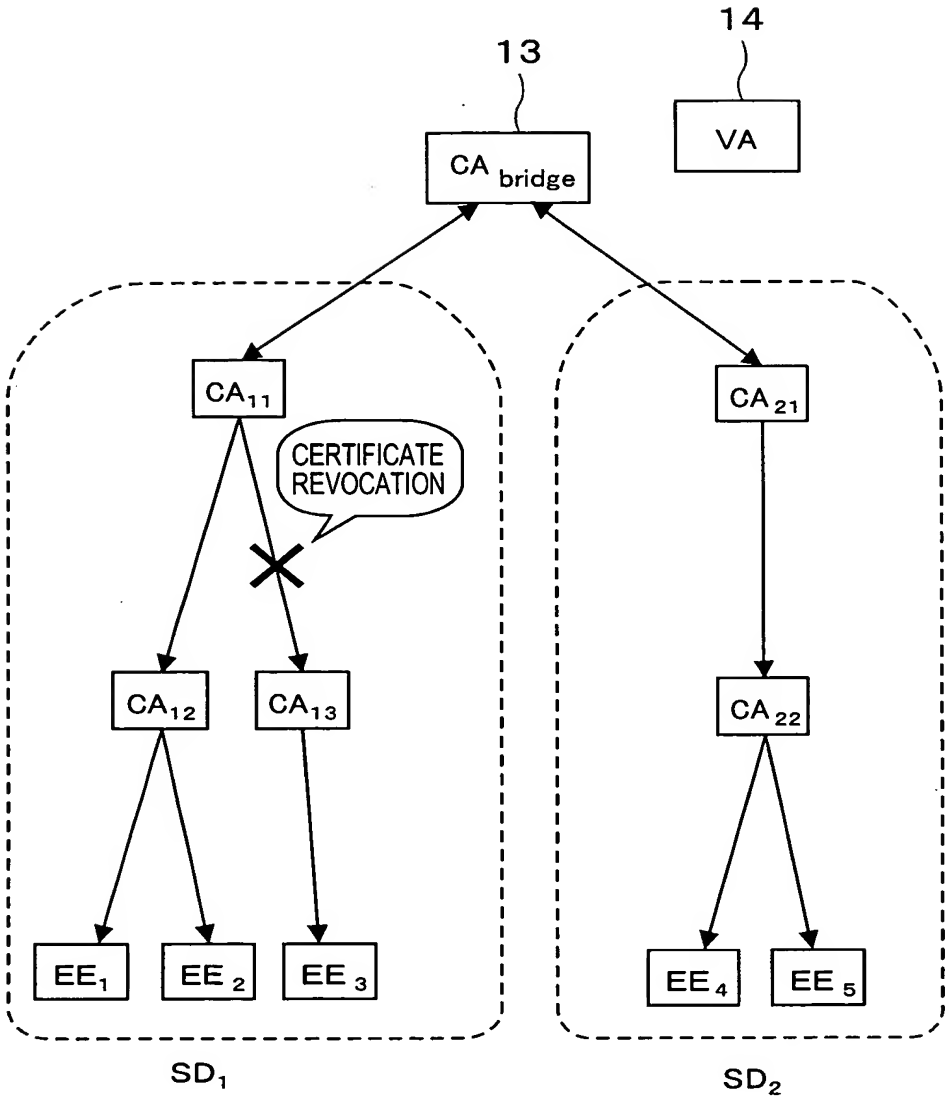

13
14
CA bridge
VA
CA11
CERTIFICATE REVOCATION
CA21
CA12
CA13
CA22
EE1
EE2
EE3
EE4
EE5
SD1
SD2

FIG.3

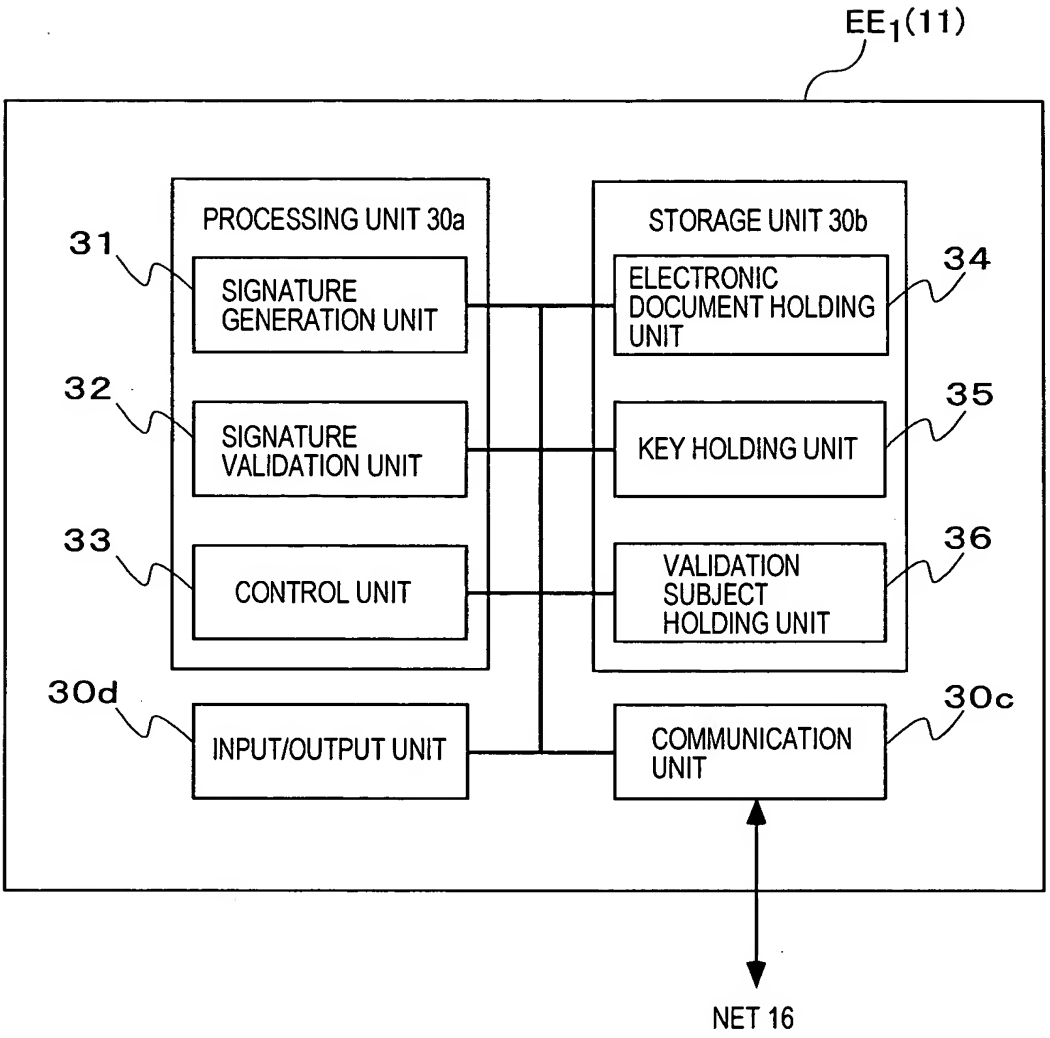

EE1(11)
PROCESSING UNIT 30a
STORAGE UNIT 30b
31
SIGNATURE GENERATION UNIT
34
ELECTRONIC DOCUMENT HOLDING UNIT
32
SIGNATURE VALIDATION UNIT
35
KEY HOLDING UNIT
33
CONTROL UNIT
36
VALIDATION SUBJECT HOLDING UNIT
30d
INPUT/OUTPUT UNIT
30c
COMMUNICATION UNIT
NET 16

FIG.4

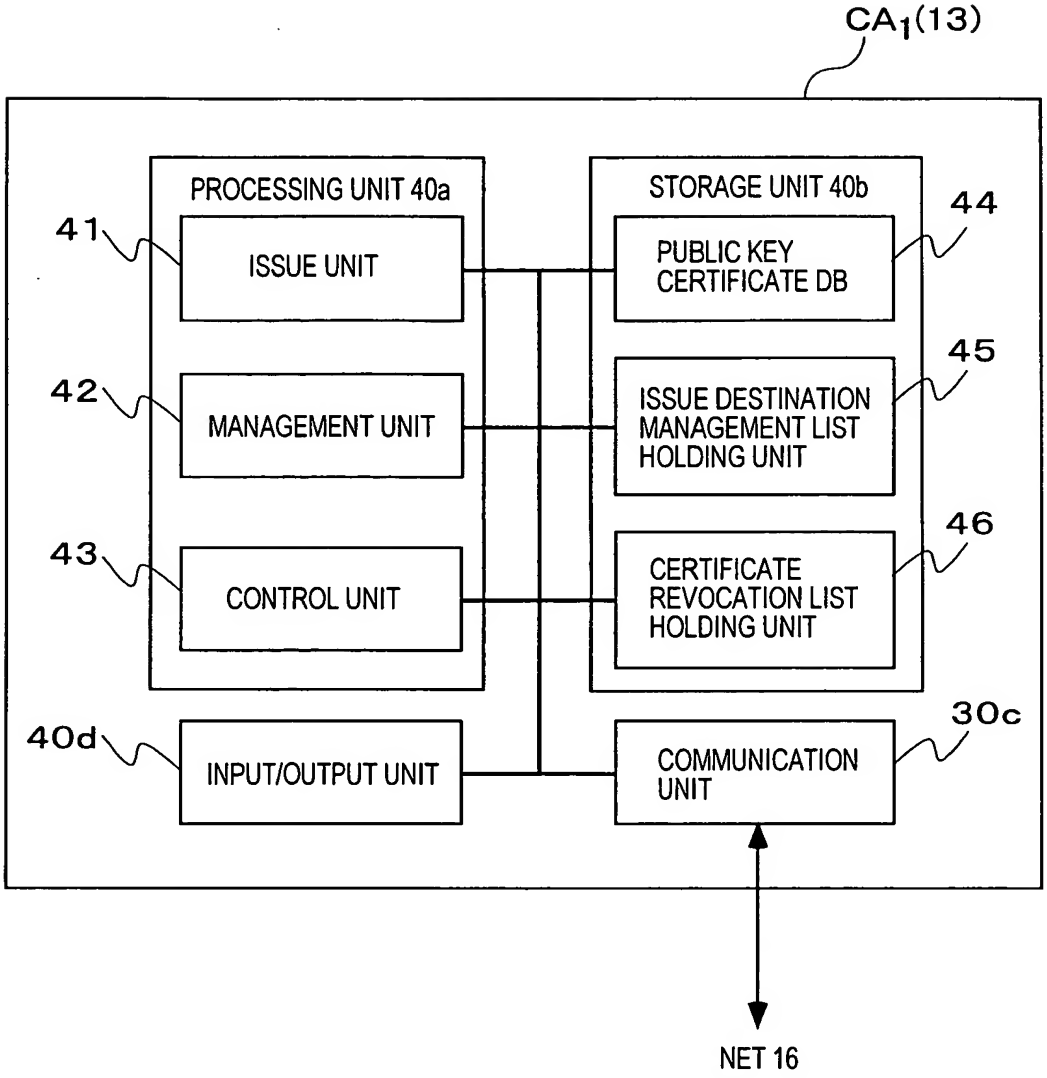

CA1(13)
PROCESSING UNIT 40a
STORAGE UNIT 40b
41
ISSUE UNIT
42
MANAGEMENT UNIT
43
CONTROL UNIT
40d
INPUT/OUTPUT UNIT
44
PUBLIC KEY CERTIFICATE DB
45
ISSUE DESTINATION MANAGEMENT LIST HOLDING UNIT
46
CERTIFICATE REVOCATION LIST HOLDING UNIT
30c
COMMUNICATION UNIT
NET 16

FIG.5

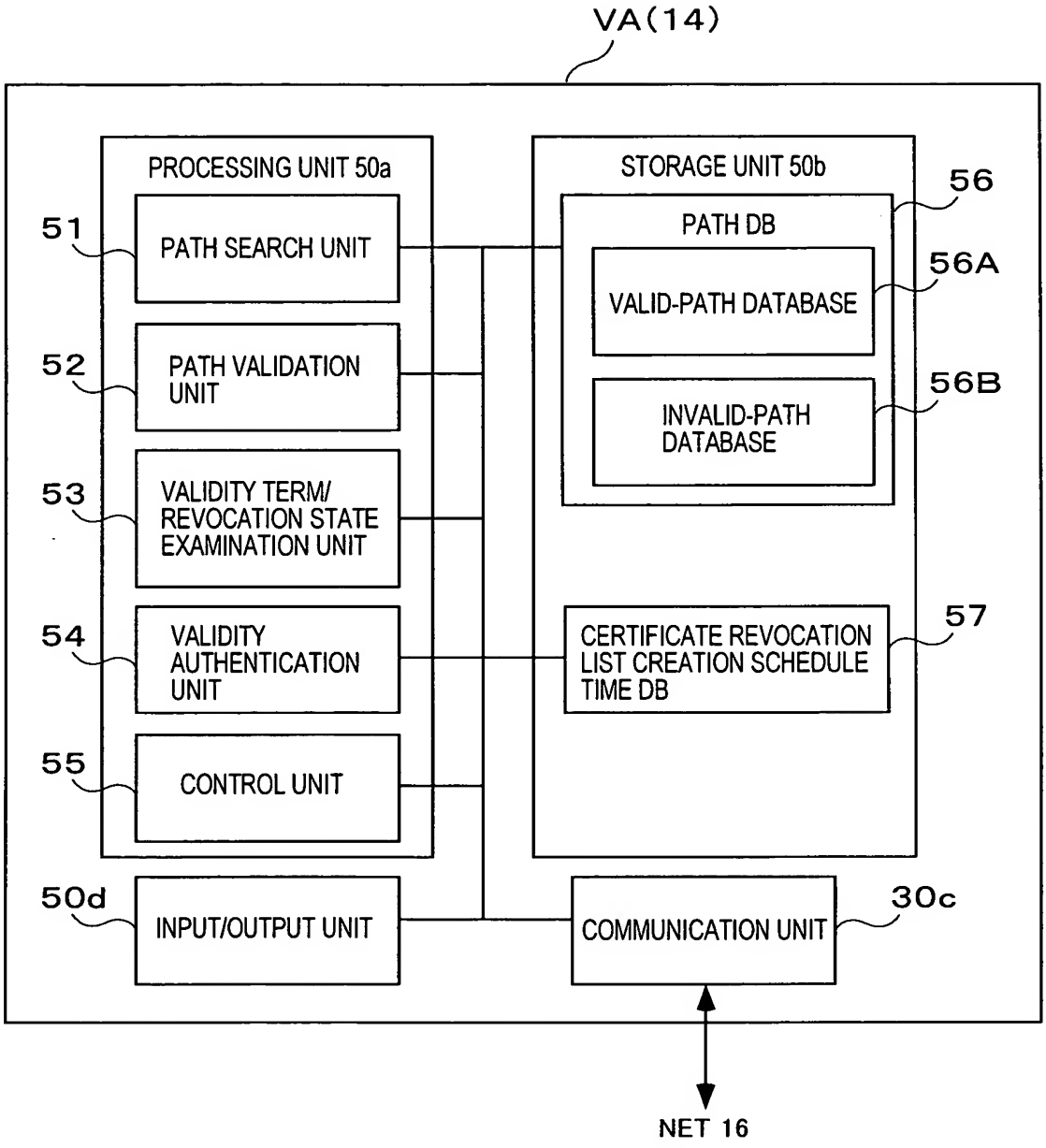

VA(14)
PROCESSING UNIT 50a
STORAGE UNIT 50b
51
PATH SEARCH UNIT
52
PATH VALIDATION UNIT
53
VALIDITY TERM/ REVOCATION STATE EXAMINATION UNIT
54
VALIDITY AUTHENTICATION UNIT
55
CONTROL UNIT
50d
INPUT/OUTPUT UNIT
56
PATH DB
56A
VALID-PATH DATABASE
56B
INVALID-PATH DATABASE
57
CERTIFICATE REVOCATION LIST CREATION SCHEDULE TIME DB
30c
COMMUNICATION UNIT
NET 16

FIG.6

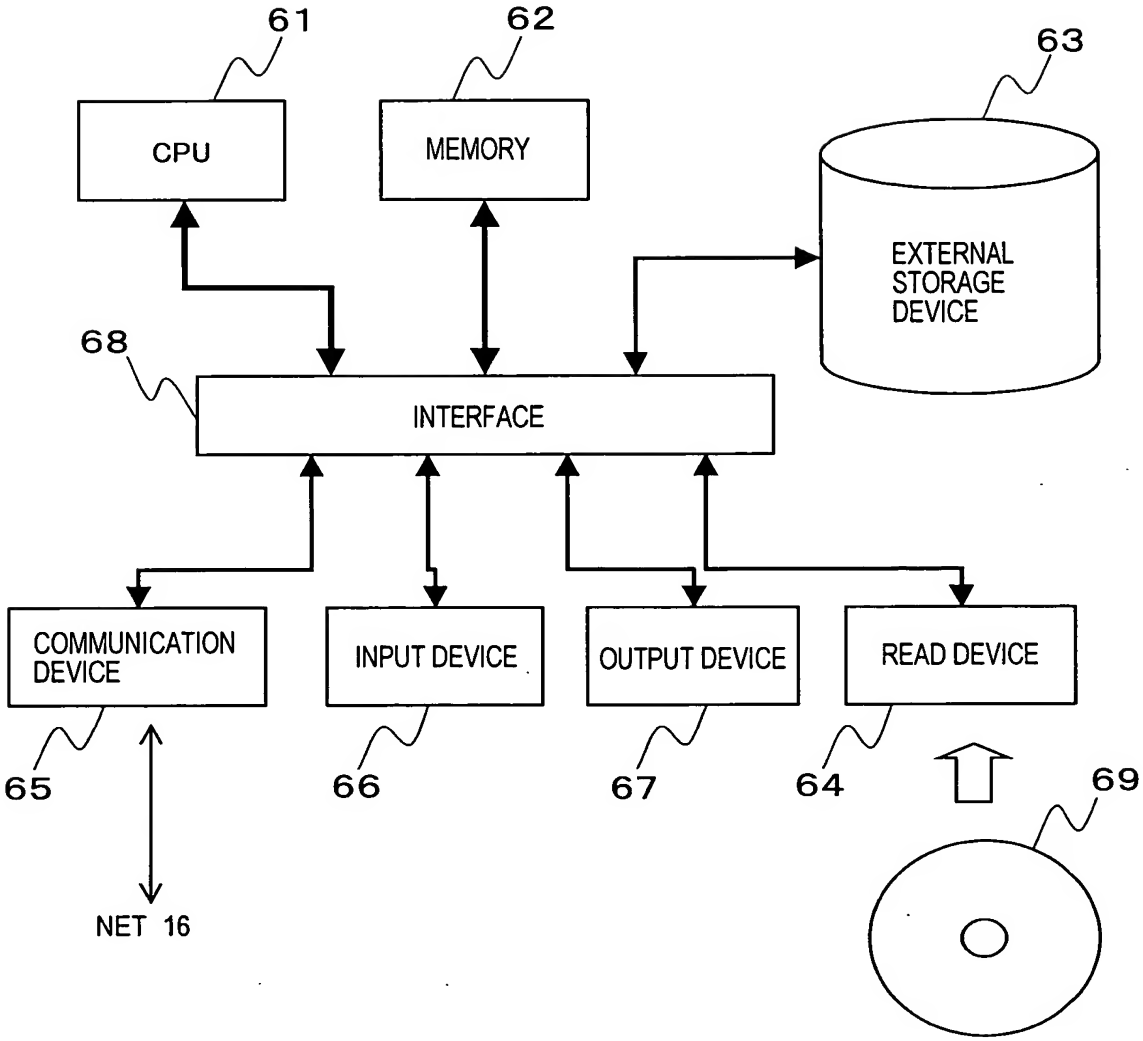

61
62
63
CPU
MEMORY
EXTERNAL STORAGE DEVICE
68
INTERFACE
COMMUNICATION DEVICE
INPUT DEVICE
OUTPUT DEVICE
READ DEVICE
65
66
67
64
69
NET 16

FIG.7

OPERATION OF SEARCHING FOR, VALIDATING AND MANAGING PATHS

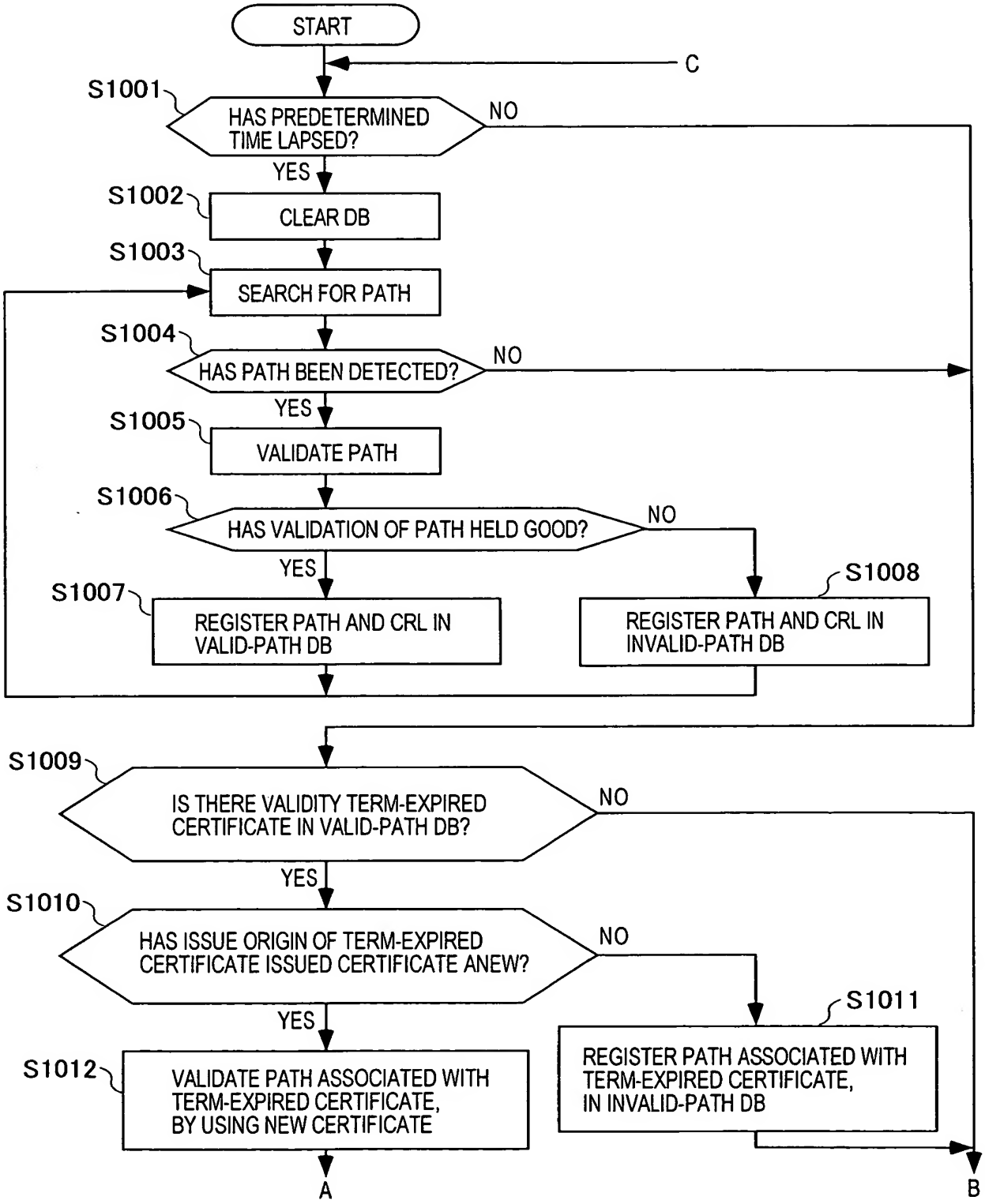


FIG.8

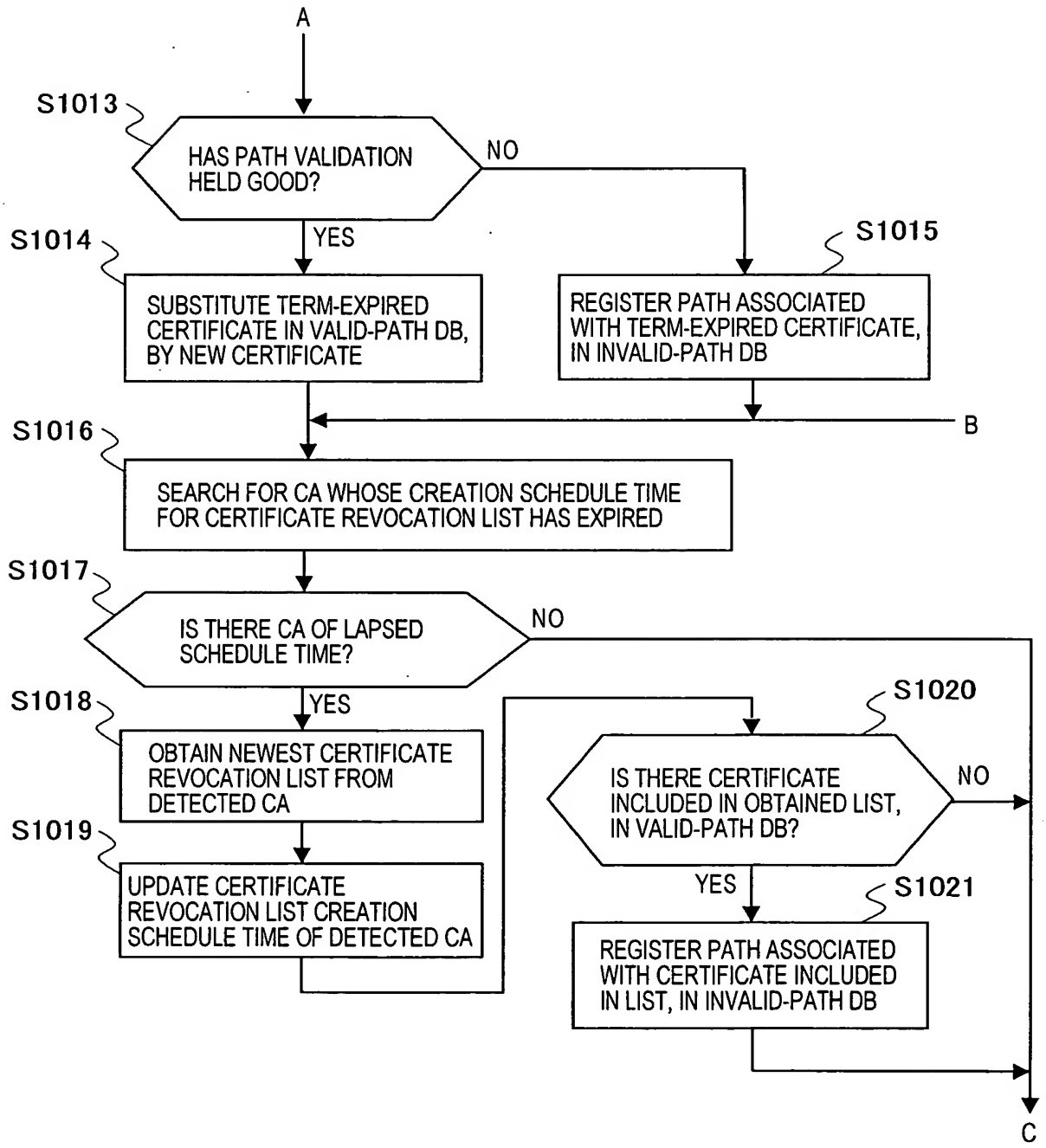

OPERATION OF SEARCHING FOR, VALIDATING AND MANAGING PATHS
A
S1013
HAS PATH VALIDATION HELD GOOD?
NO
YES
S1014
SUBSTITUTE TERM-EXPIRED CERTIFICATE IN VALID-PATH DB, BY NEW CERTIFICATE
S1015
REGISTER PATH ASSOCIATED WITH TERM-EXPIRED CERTIFICATE, IN INVALID-PATH DB
B
S1016
SEARCH FOR CA WHOSE CREATION SCHEDULE TIME FOR CERTIFICATE REVOCATION LIST HAS EXPIRED
S1017
IS THERE CA OF LAPSED SCHEDULE TIME?
NO
YES
S1018
OBTAIN NEWEST CERTIFICATE REVOCATION LIST FROM DETECTED CA
S1019
UPDATE CERTIFICATE REVOCATION LIST CREATION SCHEDULE TIME OF DETECTED CA
S1020
IS THERE CERTIFICATE INCLUDED IN OBTAINED LIST, IN VALID-PATH DB?
NO
YES
S1021
REGISTER PATH ASSOCIATED WITH CERTIFICATE INCLUDED IN LIST, IN INVALID-PATH DB
C

FIG.9

PATH SEARCH RESULT (IN CASE OF FIG. 2)

VALID PATH			
TRUST ANCHOR CA	EE CERTIFICATE ISSUING CA	PATH	CRL
CA_{11}	CA_{12}	CA_{11} - CA_{12}	VALID
	CA_{22}	CA_{11}-CAbridge-CA_{21}-CA_{22}	VALID
CA_{21}	CA_{12}	CA_{21}-CAbridge-CA_{11}-CA_{12}	VALID
	CA_{12}	CA_{21} - CA_{22}	VALID
CAbridge	CA_{22}	CAbridge-CA_{11}-CA_{12}	VALID
	CA_{12}	CAbridge-CA_{21}-CA_{22}	VALID

INVALID PATH			
TRUST ANCHOR CA	EE CERTIFICATE ISSUING CA	PATH	CRL
CA_{11}	CA_{13}	CA_{11} - CA_{12}	INVALID
CA_{21}	CA_{12}	CA_{21}-CAbridge-CA_{11}-CA_{12}	INVALID
CAbridge	CA_{12}	CAbridge-CA_{11}-CA_{12}	INVALID

FIG.10

OPERATION OF AUTHENTICATING VALIDITY OF PUBLIC KEY CERTIFICATE

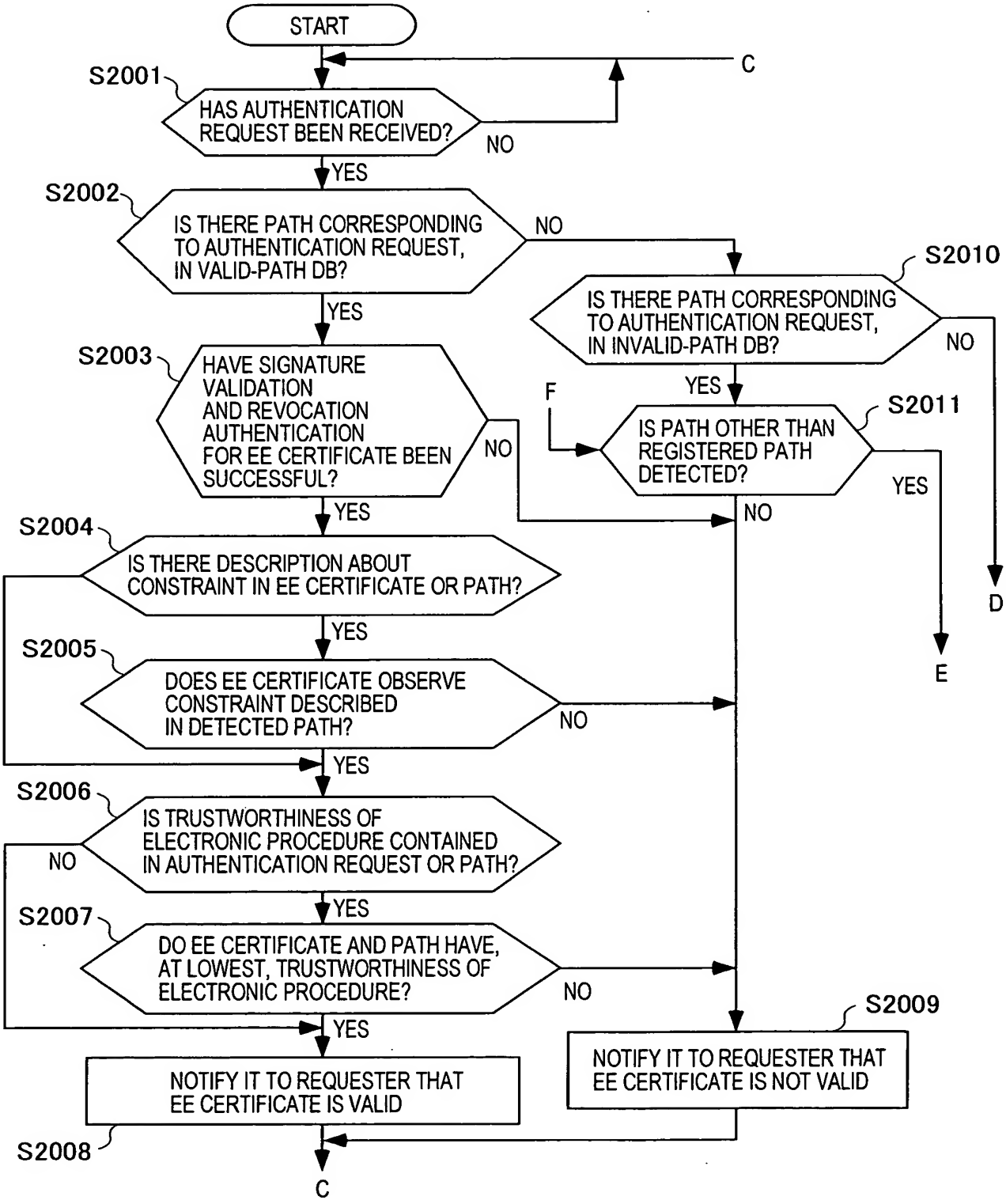


FIG.11

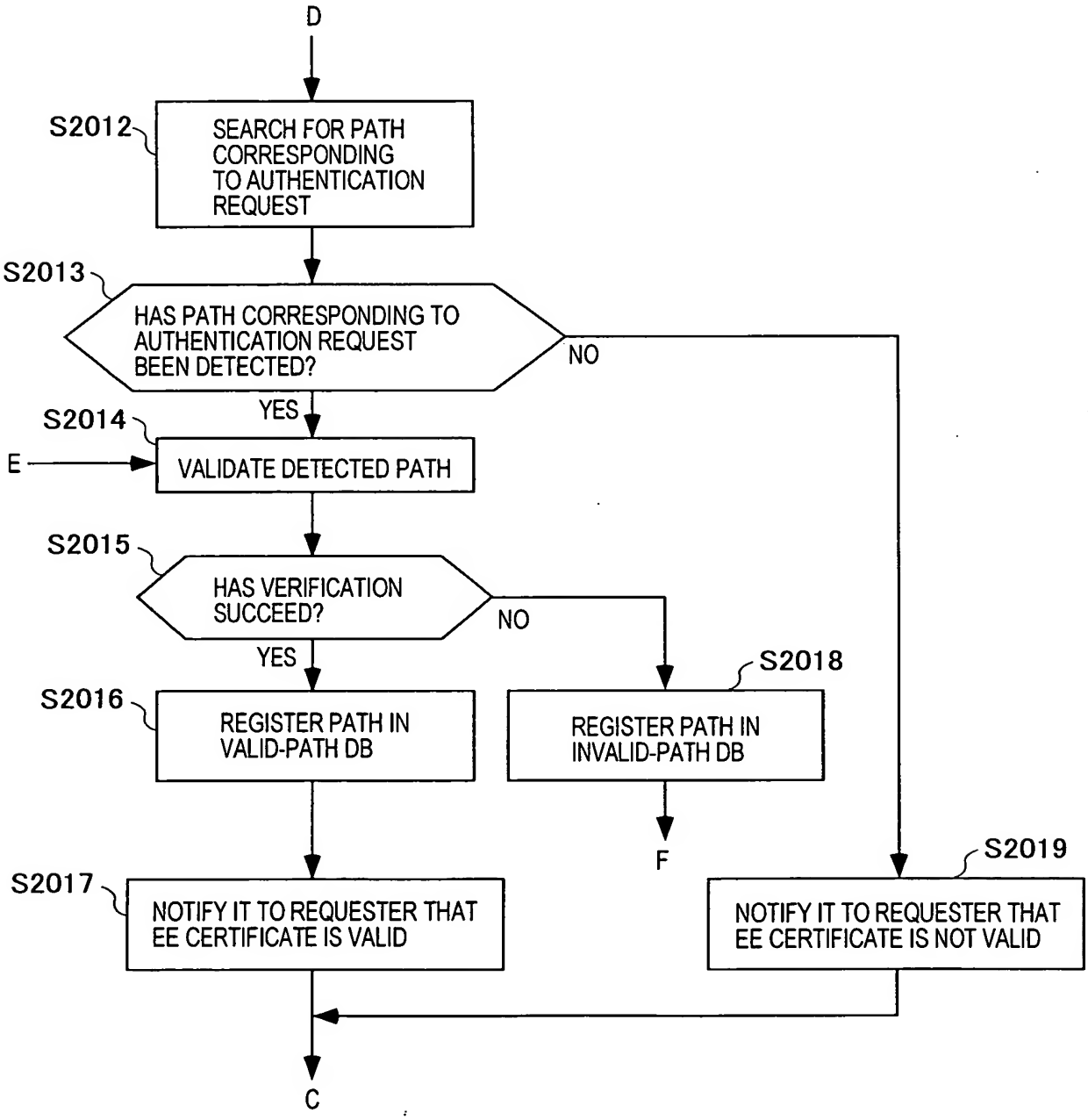
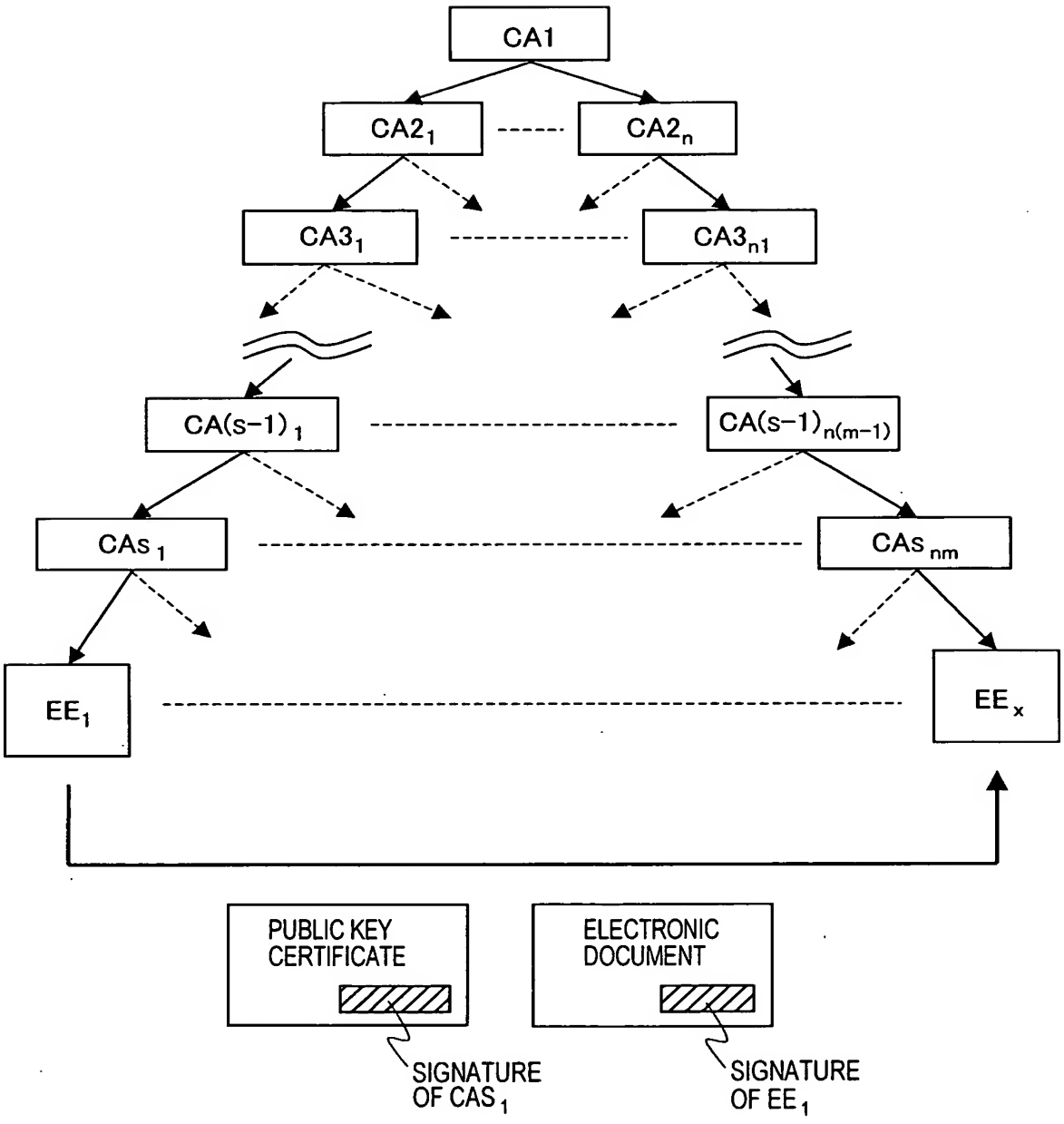

OPERATION OF AUTHENTICATING VALIDITY OF PUBLIC KEY CERTIFICATE
D
S2012
SEARCH FOR PATH CORRESPONDING TO AUTHENTICATION REQUEST
S2013
HAS PATH CORRESPONDING TO AUTHENTICATION REQUEST BEEN DETECTED?
NO
YES
S2014
E
VALIDATE DETECTED PATH
S2015
HAS VERIFICATION SUCCEED?
NO
YES
S2018
S2016
REGISTER PATH IN VALID-PATH DB
REGISTER PATH IN INVALID-PATH DB
F
S2019
S2017
NOTIFY IT TO REQUESTER THAT EE CERTIFICATE IS VALID
NOTIFY IT TO REQUESTER THAT EE CERTIFICATE IS NOT VALID
C

FIG.12


CA1
CA2 1
CA2 n
CA3 1
CA3 n1
CA(s−1) 1
CA(s−1) n(m−1)
CAs 1
CAs nm
EE 1
EE x
PUBLIC KEY CERTIFICATE
ELECTRONIC DOCUMENT
SIGNATURE OF CAS 1
SIGNATURE OF EE 1